CLAIMS:

Please amend the claims as follows:

1. (Currently Amended) A method in a computer-based environment for preparing content to be deployed on a target wireless device, comprising:

determining whether pre-provisioned content corresponding to the target wireless device exists;

where the pre-provisioned content exists, determining whether the pre-provisioned content is stored with a trusted third party host, and where the pre-provisioned content is stored with the trusted third party host, retrieving the pre-provisioned content from the trusted third party host, and providing the pre-provisioned content to the target wireless device without additional provisioning; and

where the pre-provisioned content is unavailable, selecting content from remotely stored, untrusted applications and provisioning the content for the target wireless device, wherein the provisioning comprises intercepting the content and inspecting the content, wherein the inspecting comprises at least one of examining the content to detect malicious code, determining whether the content contains banned code, and determining whether the content contains designated API; verifying that the target wireless device supports execution of the content by comparing the device capabilities to the content requirements; and providing ~~the~~ verified and provisioned content to the target wireless device;

wherein the provisioning comprises inspecting the content, wherein inspecting the content comprises an operation selected from the group consisting of deconstructing a structure of the content, checking for malicious code, checking for banned code, determining the applicable application of filters, and checking a number of activated threads;

wherein the determining the applicable application of filters comprises retrieving an application filter relevant for potential targets under examination, wherein the application filter detects one of package and

method names, package and method classes, package and method fields, API suspected to have intrusive behavior, API suspected to have malicious behavior and API that are unauthorized for use.

2. (Previously Presented) The method of claim 1, further comprising causing the prepared content to download to the target wireless device over a wireless transmission medium.
3. (Original) The method of claim 2 wherein the content is requested by a subscriber of a carrier to the computer-based environment over a wireless transmission medium.
4. (Original) The method of claim 1 wherein the provisioning comprises at least one of: inspecting the content; optimizing the content; and instrumenting the content.
5. (Canceled)
6. (Previously Presented) The method of claim 5 wherein the inspecting further comprises determining whether the application contains designated API, wherein the API is at least one of packages, classes, methods, and fields.
7. (Canceled)
8. (Previously Presented) The method of claim 4 wherein the provisioning comprises inspecting the content, wherein the inspecting is performed using an application filter, wherein the application filter specifies a list of criteria to be filtered and a target.
9. (Original) The method of claim 8 wherein the criteria is an API.
10. (Original) The method of claim 8 wherein that target is at least one of a specified client, device type, content identifier, and global definition.
11. (Previously Presented) The method of claim 4 wherein the provisioning comprises optimizing the content, wherein the optimizing comprises at least one of: reducing the size of variable names; modifying instructions to more efficient instructions; mapping executable paths in code; and removing unused code.
12. (Previously Presented) The method of claim 4 wherein the provisioning comprises instrumenting the content, wherein the instrumenting comprises inserting code that implements at least one of a billing policy, a usage policy, a notification, and an automatic content update mechanism.

13. (Previously Presented) The method of claim 1 wherein the verifying that the device supports execution of the content further comprises identifying a device, accessing capabilities of the device from a device profile, accessing device requirements of the content, and determining whether resources required by the content are available according to the device profile.
14. (Previously Presented) The method of claim 13 wherein the device profile contains information relevant to the capabilities of the device, wherein the information relevant to the capabilities of the device are selected from the group consisting of memory capacity, processor type, processing speed, and maximum size of a downloadable application.
15. (Previously Presented) The method of claim 12 wherein the billing policy comprises at least one of subscription based billing, trial use, download based billing, transmission based billing, and prepaid billing.
16. (Previously Presented) The method of claim 15 wherein the billing policy is provided by a wireless carrier infrastructure.
17. (Previously Presented) The method of claim 1 wherein the content is provisioned for a requestor, and the verifying further comprising at least one of: comparing the API used by the content to the API supported by the target wireless device and determining whether the requestor is authorized to use the content.
18. (Previously Presented) The method of claim 17 wherein determining whether the requestor is authorized determines whether the requestor has sufficient funds in a prepaid billing account to use the content.
19. (Original) The method of claim 1 wherein the verification is accomplished using profile management.
20. (Original) The method of claim 19 wherein the profile management defines profiles for at least one of a subscriber, device type, and content.
21. (Original) The method of claim 1 wherein the content is Java-based.
22. (Original) The method of claim 1 wherein the environment is integrated with a wireless carrier infrastructure.
23. (Original) The method of claim 1 wherein the content preparation provides walled-garden provisioning.

24. (Original) The method of claim 1, the computer-based environment including a network, wherein the provisioning supports the designation of the content to be prepared through browsing to a location on the network.
25. (Original) The method of claim 1 wherein the network is the Internet.
26. (Previously Presented) The method of claim 1 wherein the preparation process takes into account preferences of a requestor of the content.
27. (Original) The method of claim 1 wherein attributes that control the provisioning are specified through website administration.
28. (Previously Presented) The method of claim 1 wherein the provisioning comprises preparing an initial list of available applications.
29. (Original) The method of claim 1 wherein the content contains at least one of text, graphics, audio, and video.
30. (Currently Amended) A network-based transmission system operable in conjunction with at least one computer processor comprising:
a provisioning manager operable to control the at least one computer processor and being configured to determine whether pre-provisioned content corresponding to a requesting device exists, and where pre-provisioned content exists, to determine whether the pre-provisioned content is stored with a trusted, third party application provider;
a deployment manager operable to control the at least one computer processor and being configured to retrieve an application, and where the pre-provisioned content is stored with the trusted, third party application provider to retrieve the pre-provisioned content from the trusted, third party application provider and to deploy the pre-provisioned content without additional provisioning, and otherwise to retrieve an application from untrusted, third party hosts; and
an inspector operable to control the at least one computer processor, wherein when the application is retrieved from an untrusted, third party host, the inspector is configured to control the at least one computer processor to examine the application by a method selected from the group consisting of examining the application to detect malicious code, performing a class analysis of the

application to verify that classes in the application conform to desired standards, and applying application filters to the application;

wherein the examining comprises inspecting the content, wherein inspecting the content comprises an operation selected from the group consisting of deconstructing a structure of the content, checking for malicious code, checking for banned code, determining the applicable application of filters, and checking a number of activated threads;

wherein the determining the applicable application of filters comprises retrieving an application filter relevant for potential targets under examination, wherein the application filter detects one of package and method names, package and method classes, package and method fields, API suspected to have intrusive behavior, API suspected to have malicious behavior and API that are unauthorized for use.

31. (Previously Presented) The transmission system of claim 30 wherein the application is transmitted to the target wireless device.
32. (Previously Presented) The transmission system of claim 30, further comprising at least one of an optimizer and an instrumentation analyzer, operable with the at least one computer processor, wherein the optimizer is configured to reduce a code size of the application when possible, and wherein the instrumentation analyzer is configured to modify code in the application according to specified policies.
33. (Previously Presented) The transmission system of claim 30 wherein the desired standards are selected from the group consisting of number of API calls, type of API call, and frequency of API calls.
34. (Canceled)
35. (Previously Presented) The transmission system of claim 30 wherein the application filters comprise dynamically specifiable filters, operable with the at least one computer processor, wherein the dynamically specifiable filters specify a list of criteria to be filtered and a target.
36. (Previously Presented) The transmission system of claim 32 wherein the instrumentation analyzer is configured to cause the at least one computer processor to insert code into the application, the code being configured to

implement at least one of a billing policy, usage policy, notification, and automated content update mechanism.

37. (Canceled)

38. (Canceled)

39. (Previously Presented) The transmission system of claim 30, wherein the provisioning manager is configured to cause the at least one computer processor to verify whether a target wireless device supports execution of the application by a method selected from the group consisting of determining at least one of a user of the target wireless device is authorized to receive the application, determining whether the target wireless device supports an API used by the application, and determining whether the application has not been banned.

40. (Previously Presented) The transmission system of claim 30, wherein the provisioning manager is configured to cause the at least one computer processor to verify whether a device supports execution of the application by identifying the device, accessing capabilities of the device from a device profile, accessing device requirements of the application, and determining whether resources required by the application are available according to the device profile.

41. (Previously Presented) The transmission system of claim 30 wherein the at least one computer processor is coupled to a wireless carrier infrastructure.

42. (Previously Presented) The transmission system of claim 30 wherein the application is Java-based.

43. (Previously Presented) The transmission system of claim 30 wherein the deployment manager is coupled to the Internet.

44. (Previously Presented) The transmission system of claim 30 wherein the application contains at least one of text, graphics, audio, and video.

45. (Currently Amended) A mobile applications system operable in conjunction with a computer processor, the mobile applications system comprising a system application operable to control a computer processor to determine whether pre-provisioned content corresponding to a target device exists, and where it does not, prepare content for deployment on the target device, such that when the pre-provisioned content exists the computer processor determines whether the pre-

provisioned content is stored with a trusted, third party application provider and fetches the pre-provisioned content from the trusted, third party application providers, and when the pre-provisioned content does not exist, to fetch a retrieved application from and untrusted, third party host;

wherein where the pre-provisioned content is stored from the trusted third party application provider, the system application is configured to deliver the pre-provisioned content without additional provisioning; and otherwise to

examine the retrieved application by a method selected from the group consisting of examining the retrieved application to detect malicious code, performing a class analysis of the retrieved application to verify that classes in the retrieved application conform to desired standards, and applying application filters to the retrieved application; and verify that the target device supports execution of the retrieved application without executing the retrieved application on the device;

wherein the examining comprises inspecting the content, wherein inspecting the content comprises an operation selected from the group consisting of deconstructing a structure of the content, checking for malicious code, checking for banned code, determining the applicable application of filters, and checking a number of activated threads;

wherein the determining the applicable application of filters comprises retrieving an application filter relevant for potential targets under examination, wherein the application filter detects one of package and method names, package and method classes, package and method fields, API suspected to have intrusive behavior, API suspected to have malicious behavior and API that are unauthorized for use.

46. (Previously Presented) The mobile applications system of claim 45 wherein the target device is a wireless device.

47. (Previously Presented) The mobile applications system of claim 45 wherein the system application causes the retrieved application to be downloaded to the target device over a wireless transmission medium.

48. (Previously Presented) The mobile applications system of claim 45 wherein the retrieved application is at least one of optimized and instrumented.

49. (Previously Presented) The mobile applications system of claim 48 wherein the system application causes the computer processor to determine whether the retrieved application contains an element selected from the group consisting of malicious code; banned code; and designated API.
50. (Previously Presented) The mobile applications system of claim 48 wherein the system application causes the computer processor to apply an application filter to the retrieved application.
51. (Previously Presented) The mobile applications system of claim 48 wherein the system application causes the computer processor to insert code that implements at least one of a billing policy, a usage policy, a notification, and an automatic content update mechanism.
52. (Canceled)
53. (Canceled)
54. (Canceled)
55. (Previously Presented) The mobile applications system of claim 45 wherein the system application causes the computer processor to compare an API used by the retrieved application to an API supported by the target device; determine whether the requestor is authorized to use the content; and determine whether the content is banned.
56. (Previously Presented) The mobile applications system of claim 55 wherein the requestor is authorized where the requestor has sufficient funds in a prepaid billing account to use the retrieved program.
57. (Canceled)
58. (Previously Presented) The mobile applications system of claim 45 wherein the retrieved application is Java-based.
59. (Canceled)
60. (Previously Presented) The mobile applications system of claim 45 wherein the content contains at least one of text, graphics, audio, and video.
61. (Currently Amended) A computer-based content deployment system for one of delivering pre-provisioned content or provisioning retrieved content for a target device, operable with a computer and comprising:

a verification manager that causes the computer to verify that the retrieved content is authorized and the target device supports resources needed by the retrieved content;

a deployment manager coupled to and operational with both the verification manager and the computer, the deployment manager configured to retrieve content from at least trusted, third party application providers, and untrusted, third party hosts;

an inspector, coupled to and operational with the verification manager and deployment manager and the computer, wherein when the content is retrieved from an untrusted, third party host, the inspector examines the retrieved content by a method selected from the group consisting of examining the retrieved content to detect malicious code, performing a class analysis of the retrieved content to verify that classes in the retrieved content conform to desired standards, and applying application filters to the retrieved content; and

a provisioning manager, operable with the computer, and operable with and coupled to the verification manager, the deployment manager and the inspector, that, where the content is retrieved from one or more of the untrusted, third party hosts, provisions the retrieved content according to requirements of the target device by at least one of inspecting the content, optimizing the content, and instrumenting the content, or determines whether pre-provisioned content exists, and where the pre-provisioned content exists, determines whether the pre-provisioned content is stored with a trusted, third party host, and where the pre-provisioned content is stored with the trusted third party host, retrieves the pre-provisioned content from the trusted third party host without additional provisioning;

wherein inspecting the content comprises an operation selected from the group consisting of deconstructing a structure of the content, checking for malicious code, checking for banned code, determining the applicable application of filters, and checking a number of activated threads;

wherein the determining the applicable application of filters comprises retrieving an application filter relevant for potential targets under examination, wherein the

application filter detects one of package and method names, package and method classes, package and method fields, API suspected to have intrusive behavior, API suspected to have malicious behavior and API that are unauthorized for use.

62. (Original) The deployment system of claim 61 wherein the provisioning manager further comprises at least one of: subscriber verifier; device verifier; and application verifier.
63. (Previously Presented) The deployment system of claim 62 wherein the subscriber verifier causes the computer to determine whether a subscriber of a wireless carrier service is authorized to use the retrieved content.
64. (Previously Presented) The deployment system of claim 62 wherein the device verifier causes the computer to determine whether the target device supports an API required by the retrieved content.
65. (Previously Presented) The deployment system of claim 62 wherein the application verifier causes the computer to determine whether the retrieved content is banned.
66. (Original) The deployment system of claim 61 wherein the target device is a wireless device.
67. (Original) The deployment system of claim 61 wherein the deployment system is integrated with a wireless carrier computer system.
68. (Previously Presented) The deployment system of claim 61 wherein instrumenting the retrieved content provides support for at least one of a billing policy, a usage policy, a notification, and an automatic content update mechanism.
69. (Previously Presented) The deployment system of claim 61, further comprising: a billing manager, coupled to an operable with the provisioning manager and the computer, that provides support for provisioning the retrieved content according to a billing policy.
70. (Original) The deployment system of claim 69 wherein the billing policy is one of subscription base billing, trial use, download based billing, transmission based billing, and prepaid billing.
71. (Original) The deployment system of claim 61 wherein the designation of the content to be provisioned is determining by browsing to a location on a network.

72. (Original) The deployment system of claim 61 wherein the content is Java-based.

73. (Original) The deployment system of claim 61 wherein the content contains at least one of text, graphics, audio, and video.